

GeekBrains

Урок 3 Видео 3

Криптография

Криптографические хеш-функции для хранения паролей

В этом видео

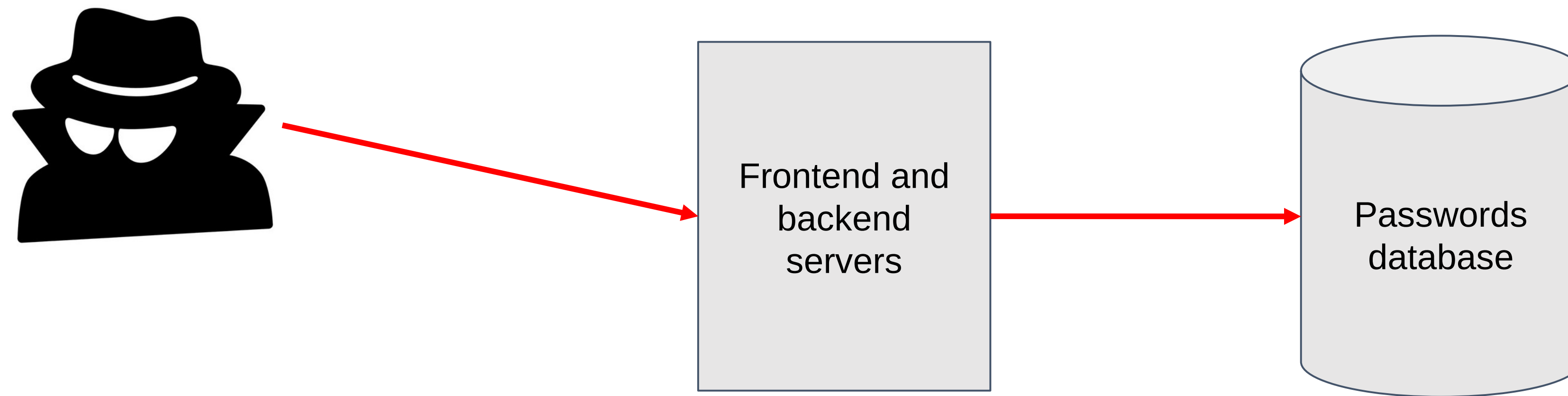
1. Современные проблемы хеширования паролей
2. bcrypt
3. Argon2, scrypt

Рост мощностей

Специализированные интегральные схемы (ASIC), видеокарты, …



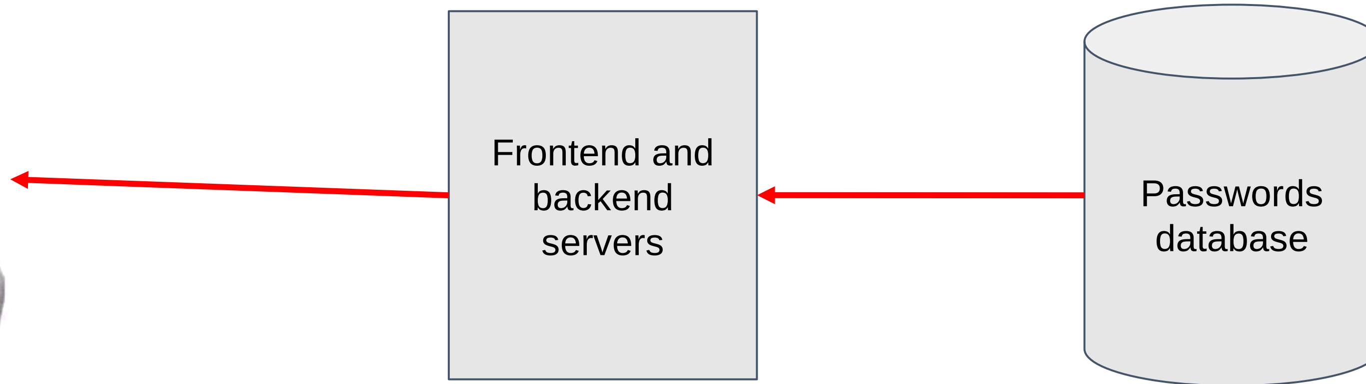
Крипто-функции для хранения паролей



$2b$16$l7a9porj89C.Afh4n8orYuQeREyxjiVOoYgLfkgRhV/NWHx9OcKam
...

Крипто-функции для хранения паролей





$2b$**16**$l7a9porj89C.Afh4n8orYuQeREyxjiV
OoYgLfkgRhV/NWHx9OcKam
…

$2b$16$l7a9porj89C.Afh4n8orYuQeREyxjiVOoYgLfkgRhV/NWHx9OcKam

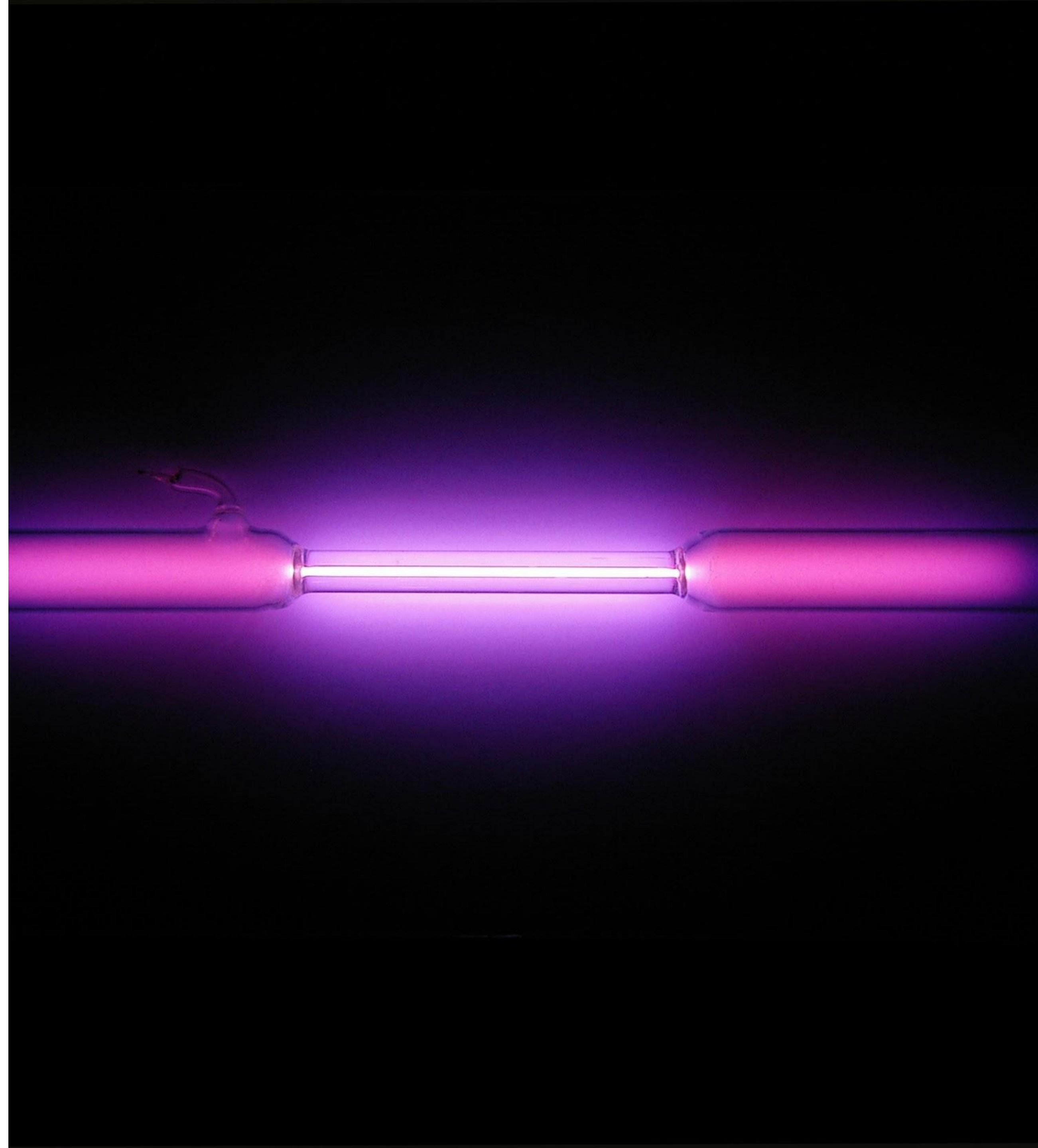
2b - версия
16 - параметр сложности вычислений

l7a9porj89C.Afh4n8orYu - соль (128 бит)

QeREyxjiVOoYgLfkgRhV/NWHx9OcKam - хеш (184 бит)

Argon2, scrypt

Увеличить расход оперативной памяти и уменьшить возможность распараллеливания



Итоги

1. Современные проблемы хеширования паролей
2. bcrypt
3. Argon2, scrypt